THE JOHNS HOPKINS
FEDERAL CREDIT UNION
Serving the Johns Hopkins community since 1971

ATTN: Identity Theft Task Force
January 19, 2007

Can you please make stronger requirements for the retailers is it relates to credit/debit card identity theft. I work for a small financial institution, Johns Hopkins Federal Credit Union ($205 million in assets) and we have to keep responding to instances where a retailer or it's processor had unscrupulous employees who compromised the card information. As with this most recent breach involving TJ Maxx and their other companies (below is the notice VISA sent financial institutions, later it was identified that it was TJ Maxx), they were responsible for the breach yet the financial institutions like ours have to take steps to review affected cards and perhaps reissue cards--costing us a lot of time and money when the fault was not ours.

I would like to see:

1) When the retailer swipes the card and the magnetic stripe is "read", the screen ideally would show the issuing financial institution name, and the consumer's name, so the retailer can see that the plastic card information matches what's on the magnetic stripe. In a previous breach, someone got our card and BIN numbers from a retailer and made new plastic with a Canadian bank's look. Fortunately a sharp Canadian retailer knew that the BIN on the card was not that bank's BIN.
2) Retailers should be required to ask for ID--again to see that when a name is on a card and on the screen as suggested above, the person presenting the card is indeed that person.

These few steps would help consumers and financial institutions. Currently the retailers are the ones violating policy and being lax, yet they are not affected.

Thank you.

Lynn M. Gregory
Sr. Vice President - Marketing and Member Services
Johns Hopkins FCU
2027 E. Monument St.
Baltimore, MD 21287
410-534-4500, x258

Visa USA Update on Retailer Data Compromise

Recently, Visa was informed of a potential large-scale data compromise at a national retailer involving all major payment card brands. While the full extent of the incident is being determined, we are providing member financial institutions with early notification so that you may begin assessing the potential effect on your portfolio and take necessary action to protect your cardholders. We are also providing resources to assist you in your communications to your cardholders.

Visa is working diligently with the compromised retailer, independent security vendors, the U.S. Secret Service, the acquirer and other card brands to conduct a thorough forensic investigation. At the request of law enforcement, we are not disclosing at this point the details of the investigation, including the name of the retailer involved.

It is important to note that information regarding data compromises may become public quickly, and your institution should be prepared to address questions from your customers. Visa will continue to provide as much additional information about this incident as possible.

Visa's focus throughout this retailer compromise is to help issuers mitigate the effect of fraud on their business. To that end, Visa will be:

* **Providing Access to Compromised Account Numbers.** As information on compromised accounts comes to Visa from the acquirer, it will be loaded into our Compromised Account Management System (CAMS), and issuers will be given access to their affected data. We are taking the extra step to delete duplicate accounts to help expedite your use of the information.

An initial CAMS alert is being sent today. Members can expect additional alerts in the coming days. Members must be registered with Visa to receive CAMS alerts. To register for CAMS, please send an e-mail to cams@visa.com.

* **Monitoring for Fraud.** Visa is loading all related accounts into its Rare Event Detection program and conducting around-the-clock monitoring for unusual spending patterns on the compromised accounts. Additionally, all transactions stemming from the affected accounts will be scored by Advanced Authorization with a condition code indicating it is part of a data compromise.

* **Assisting in Recovery.** Since October 1, 2006, Visa has offered the Account Data Compromise Recovery (ADCR) process to help issuers offset compromise-related costs. This includes partial reimbursement for magnetic-stripe counterfeit fraud transactions and the recovery of some costs related to the reissuance of cards that are part of an eligible CAMS alert.

* **Working with Merchants to Prevent Compromises.** Visa remains dedicated to helping retailers adopt the Payment Card Industry Data Security Standard (PCI DSS), which, when followed, has been highly effective in preventing data compromises from occurring. Visa's recently introduced PCI Compliance Acceleration Program (PCI CAP) is designed to speed PCI compliance and the elimination of track data storage through financial incentives and fines. Visa is currently reviewing the applicability of enforcement action related to this compromise.

* **Helping Maintain the Trust of Cardholders.** In the coming days and weeks, this incident is likely to receive significant media attention. Cardholders will likely have questions related to how they may be affected. Visa is providing a number of sample communications to help you inform your cardholders of their applicable protections. We have available a sample call center script, a cardholder letter and a statement insert that can be accessed at the links below. These materials will also be available on Visa Online (www.us.visaonline.com), where additional information is available on how to order statement inserts. Feel free to adapt materials to your financial institution's particular needs. Throughout the materials, Visa has emphasized Zero Liability protection, a highly effective message with cardholders following a compromise.

Additionally, Visa is providing you with a copy of its media response statement and a copy of the CAMS alert that your risk contacts have received if you have affected accounts.

Meanwhile, we will keep you updated on this incident as further details emerge. Please contact your Account Executive or call (888) 847-2242 if you have any questions. Thank you in advance for your partnership as we work together to maintain trust in the payment system.